ANALISA MODIFIKASI ALGORITMA RC4 MENGGUNAKAN *TWO STATE TABLES* DAN *INITIAL STATE FACTORIAL* UNTUK PENGAMANAN FILE

SKRIPSI

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana Strata 1
Teknik Informatika Universitas Muhammadiyah Malang

Barkie Hasni Azzaky
201310370311299

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2018

LEMBAR PERSETUJUAN

ANALISA MODIFIKASI ALGORITMA RC4 MENGGUNAKAN *TWO STATE TABLES* DAN *INITIAL STATE FACTORIAL* UNTUK PENGAMANAN FILE

SKRIPSI

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Teknik Informatika Universitas Muhammadiyah Malang

Disusun oleh:
BARKIE HASNI AZZAKY
201310370311299

Menyetujui,

Pembimbing I	Pembimbing II
Aminudin, S.Kom., M.Cs	**Sofyan Arifianto, S.Si., M.T**
NIDN. 0701068603	**NIDN. 0721038309**

LEMBAR PENGESAHAN

ANALISA MODIFIKASI ALGORITMA RC4 MENGGUNAKAN *TWO STATE TABLES* DAN *INITIAL STATE FACTORIAL* UNTUK PENGAMANAN FILE

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

Teknik Informatika Universitas Muhammadiyah Malang

Disusun Oleh:

BARKIE HASNI AZZAKY

201310370311299

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji pada tanggal 25 Juli 2018

Menyetujui,

Penguji I	Penguji II
Denar Regata Akbi, S.KOm, M.Kom	**Fauzi Dwi Setiawan S, S.T, M.ComSc**
NIDN. 0701058601	**NIDN. 18930706199**

Mengetahui,

Ketua Jurusan Teknik Informatika

Gita Indah Marthasari, S.T, M.Kom

NIDN. 0720038101

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Barkie Hasni Azzaky
Tempat, Tanggal Lahir	: Lamongan, 13 Desember 1993
NIM	: 201310370311299
Fakultas / Jurusan	: Teknik / Teknik Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Analisa Modifikasi Algoritma RC4 Menggunakan *Two State Tables* dan *Initial State Factorial* untuk Pengamanan File"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun keseluruhan, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko / sanksi yang berlaku.

Malang, 13 Juli 2018

Yang Membuat Pernyataan

BARKIE HASNI AZZAKY

Mengetahui,

Pembimbing I	Pembimbing II
Aminudin, S.Kom., M.Cs	**Sofyan Arifianto, S.Si., M.T**
NIDN. 0701068603	**NIDN. 0721038309**

LEMBAR PERSEMBAHAN

Sembah sujud serta syukur panjatkan kepada kehadirat Allah SWT, Dzat yang Maha Berilmu diatas mereka yang merasa diri berilmu, serta pencipta Maha Sempurna diatas segala yang dianggap sempurna. Taburan cinta dan kasih saying-Mu telah memberikan kekuatan, membekaliku dengan ilmu serta memperkenalkanku dengan cinta. Atasa karunia serta kemudahan yang Engkau berikan akhirnya skripsi yang sederhana ini dapat terselesaikan. Sholawat dan salam selalu terlimpahkan keharibaan Rosullah Muhammad SAW.

Emak dan Bapak Tercinta, sebagai tanda bukti, hormat dan rasa terima kasih yang tak terhingga kupersembahkan karya kecil ini kepada Emak dan Bapak yang telah memberi kasih sayang, segala dukungan dan cinta kasih yang tidak mungkin dapat kubalas dengan selembar kertas yang bertulisan kata cinta dan persembahan. Semoga ini menjadi langkah awal untuk membuat Emak dan Bapak bahagia karan kusadar selama ini belum bisa berbuat lebih. Untuk Emak dan Bapak yang selalu membuatku termotivasi dan selalu menyirami kasih sayang, selalu mendoakanku, selalu sabar menasehatiku menjadi lebih baik, Terima Kasih Emak.., Terima Kasih Bapak.

Untuk embak-embakku dan adikku, tiada yang paling mengharukan saat kumpul kalian, walaupun sering bertengkar tapi hal itu selalu menjadi warna yang tak akan bisa tergantikan, terimakasih atas doa dan bantuan selama ini, hanya karya kecil ini yang dapat aku persembahkan. Maaf belum bisa menjadi panutan yang baik seutuhnya, tapi aku akan menjadi yang terbaik untuk kalian semua..

Buat sahabat- sahabatku Ashabul Qohwah terimakasih banyak atas bantuan, doa, nasehat, hiburan, kekeluargaan, ojekkan, ejekkan dan semangat yang kalian berikan hingga saat ini, aku tak akan melupakan semua yang telah kalian berikan selama ini. Untuk sahabat seperjuangan seluruh sahabat kelas IT-G, terimakasih telah menjadi tempat dan sandaran saat pengerjaan tugas akhir ini sehingga dapat terselesaikan.

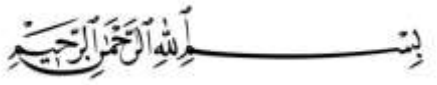
Untuk teman yang istimewa Winda Wahyu Affandini, terimakasih atas sayang, perhatian dan kesabaranmu yang telah memberikanku semangat, bantuan dan inspirasi dalam menyelesaikan tugas akhir ini. Semoga dan semoga disegerakan. Terimakasih banyak “ndook”..

Bapak Aminudin, dan Bapak Sofyan Arifianto selaku dosen pembimbing tugas akhir saya, terimakasih banyak pak..., saya sudah dibantu selama ini, sudah dinasehati, sudah diajari, saya tidak akan lupa atas bantuan dan kesabaran dari bapak. Terima kasih banyak untuk semua ilmu, didikan dan pengalaman yang sangat berarti yang telah kalian berikan kepada kami.

Seluruh pengajar di Teknik Informatika UMM yang telah mengajarkan ilmu kepada penulis dan tak akan pernah dapat dibalas oleh penulis. Bapak dan ibu dosen lah yang telah menempa diri penulis sehingga menjadi sekarang. Semoga Allah Subhanahu wa Ta'ala juga membalas seluruh jasa bapak dan ibu. Amin.

Untuk semua pihak yang tidak tersebut yang sudah membantu selama proses pengerjaan Tugas Akhir ini saya ucapkan terimakasih sebanyak banyaknya. Semoga Allah SWT membalas semua kebaikannya. Aamiin..

KATA PENGANTAR



Assalamu'alaikum Warohmatullohi. Wabarokatuh.

Syukur Alhamdulillah Segala puji bagi Allah SWT yang telah melimpahkan rahmat, taufik serta hidahNya, sehingga penulis dapat menyelesaikan skripsi yang berjudul:

"ANALISA MODIFIKASI ALGORITMA RC4 MENGGUNAKAN TWO STATE TABLES DAN INITIAL STATE UNTUK PENGAMANAN FILE"

Skripsi ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Komputer pada Jurusan Teknik Informatikaa, Fakultas Teknik Universitas Muhammadiyah Malang

Peneliti menyadari masih banyak kekurangan dan keterbatasan dalam penulisan tugas akhir ini. Untuk itu, penulis sangat mengharapkan saran yang membangun agar tulisan ini dapat berguna untuk perkembangan ilmu pengetahuan kedepan.

Malang, 13 Juli 2018

Penulis

Barkie Hasni Azzaky

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR PUSTAKA

[1] Zain, Ruri Hartika. "PERANCANGAN DAN IMPLEMENTASI CRYPTOGRAPHY DENGAN METODE ALGORITMA RC4 PADA TYPE FILE DOCUMENT DENGAN MENGGUNAKAN BAHASA PEMROGRAMAN VISUAL BASIC 6.0" Jurnal Processor Vol. 8 No. 1 2013.

[2] Jindal, Poonam dan Brahmjit Singh. "Performance Analysis of Modified RC4 Encryption Algorithm" *International Conference on Recent Advances and Innovations in Engineering (ICRAIE)* 2014.

[3] Xue, Pie, Tao Li, and Han Dong. "GB-RC4: Effective brute force attack on RC4 algorithm using GPU". *International Green and Sustainable Comuputing Conference (IGSCC)* 2016.

[4] Puspitasari, Amelia, Ari Moesriami Barmawi dan Tjokorda Agung Budi W. " Penanganan Bit Flipping Attack (BFA) pada Sistem Kriptografi RC4". Program Studi Teknik Informatika Institut Teknologi Telkom.

[5] Searan, Sura M. dan Sagheer, Ali M. " Modification of RC4 Algorithm by using Two State Table and Initiaal State Factoral" *I. J. Computer Network and Information Security (IJCNIS)* 2016.

[6] Sadikin, Rifki. 2012. "*Kriptografi Untuk Keamanan Jaringan dan Implementasinya Dalam Bahasa Java"*. Yogyakarta: CV ANDI OFFSET.

[7] Ariyus, Dony. 2005. "*Kriptografi Keamaman Data dan Komunikasi"*. Penerbit: GRAHA ILMU.

[8] Ariyus, Dony. 2008. "*Pengantar Ilmu Kriptografi : Teori Analisis dan Implementasi*". Yogyakarta: CV ANDI OFFSET.

[9] Arintamy, Vivien Septyaningttyas, Cahyani, Niken Dwi Wahyu dan Mulyana , Asep " ANALISIS ALGORITMA RC4 SEBAGAI METODE ENKRIPSI WPA-PSK PADA SISTEM KEAMANAN JARINGAN WIRELESS LAN" *e.Proceeding of Enginering: Vol.1 No.1* 2014.

[10] Hammod, M. M., K. Yoshigoe, and A. M. Sagheer. "RC4-2S: RC4 Stream Cheaper with Two State Tables". *Information Technology Converence,* Lecture Notes in Electrical Engineering. 2013

[11] Fithria, Naila. "Jenis-Jenis Serangan terhadap kriptografi" *Teknik Informatika Institut Teknologi Bandung*. 2017.

BIOGRAFI PENULIS

Nama	:	Barkie Hasni Azzaky
NIM	:	201310370311299
TTL	:	Lamongan, 13 Desember 1993
Alamat Asal	:	Sidomukti Brondong Lamongan
Email	:	zacky.vengeance.zv@gmail.com
No. HP	:	081336334948

No	Nama Sekolah	Mulai	Sampai
1.	SD Negeri Sidomukti	1999	2006
2.	SMPM 12 Sendangagung	2006	2009
3.	MA Al-Ishlah Paciran	2009	2012
4.	Universitas Muhammadiyah Malang	2013	2018